

### REMARKS

Claims 1, 2, 5, 6, 9, 10, and 13-63 were pending in the present application. Applicant amends Claims 9, 13, 30, and 47 to clarify claimed subject matter and/or correct informalities. The original specification and drawings support these claim amendments at least at pages 7, 9-13, 23-26, and Figures 2 and 4. Therefore, these revisions introduce no new matter. Claims 16, 33, and 50 have been cancelled without prejudice.

Claims 1, 2, 5, 6, 9, 10, 13-15, 17-32, 34-46, and 48-63 are for consideration upon entry of the present Amendment. Applicant requests favorable reconsideration of this response and allowance of the subject application based on the following remarks.

#### *Previous Claims Rejections Under 35 USC § 101*

Applicant appreciates Examiner's withdrawal of the 35 U.S.C. §101 rejections in the previous Office Action.

#### *Claim Rejections under 35 U.S.C. §103*

A. Claims 1, 2, 5, 6, 9, 10, 13-15, 29-32, 46-49, and 63 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 45, NO. 5, JULY 1999; Pages 1717-1719 (hereinafter "Frey") in view of Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves".

**B. Claims 16-28, 33-45, and 50-62** stand rejected under 35 U.S.C. §103(a) as being unpatentable over Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems" IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 45, NO. 5, JULY 1999; Pages 1717-1719 (hereinafter "Frey1") in view of Non-Patent Literature to Gerhard Frey, Michael Muller, and Hans-Georg Ruck; "Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves", (hereinafter "Frey2") and further in view of Non-Patent Literature to Barreto et al., entitled "Efficient Algorithms for Pairing-Based Cryptosystems". Applicant respectfully traverses the rejection.

**Claims 1, 2, 5, 6, 9, 10**

Independent Claim 1 recites a method comprising:

- determining at least one Squared Tate pairing for at least one hyperelliptic curve;
- wherein determining the Squared Tate pairing further includes:
  - forming a mathematical chain for  $m$ , wherein  $m$  is a positive integer and an  $m$ -torsion element  $D$  is fixed on Jacobian of the hyperelliptic curve  $C$ ;**
  - wherein the mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain;**
  - cryptographically processing selected information based on the determined Squared Tate pairing;
  - outputting validation of selected information based on the determined Squared Tate pairing; and
  - determining a course of action in response to validation of selected information.

Applicant respectfully submits that no such method for is taught or suggested by Frey1 and Frey2.

### References Fail to Teach or Suggest a Mathematical Chain

First, Applicant asserts the Office has failed to establish a *prima facie* case of obviousness. Frey1 fails to teach or suggest “forming a mathematical chain for  $m$ , wherein  $m$  is a positive integer and an  $m$ -torsion element  $D$  is fixed on Jacobian of the hyperelliptic curve  $C$ ”, as recited in Applicant’s Claim 1.

Frey1 is directed towards Tate pairing on Abelian varieties in Lichtenbaum’s version (page 1717, right column). The Office cites  $m=p^k$  which illustrates  $p$  is an odd prime number and  $p^1$  is the exact  $p$ -power dividing  $\#E(F_q)$  (page 1718, right column, Remark 2.4). Applicant respectfully disagrees. In contrast, Applicant’s Claim 1 recites “forming a mathematical chain for  $m$ , wherein  $m$  is a positive integer and an  $m$ -torsion element  $D$  is fixed on Jacobian of the hyperelliptic curve  $C$ ”. These are not the same features. Thus, Frey1 fails to teach or suggest the recited features of Applicant’s Claim 1.

Frey2 fails to compensate for the deficiencies of Frey1. Frey2 mentions determining all linear combinations of a finite set of elements...reducing to the computation of the discrete logarithm (Abstract). In contrast, Applicant’s Claim 1 recites “wherein the mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain”. These are not similar in function. Rather Frey2 mentions reducing to the computing, not an addition chain and an addition-subtraction chain. Thus, Frey2 does not provide what is missing from Frey1 to support a §103 rejection.

Frey1 and Frey2, alone or in combination, do not teach or suggest “forming a mathematical chain for  $m$ , wherein  $m$  is a positive integer and an  $m$ -torsion element  $D$  is

fixed on Jacobian of the hyperelliptic curve  $C$ ; and wherein the mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain”, as recited in Applicant’s Claim 1. Accordingly, Applicant submits that the evidence relied upon by the Office does not support the rejections made under §103(a).

**Independent Claims 5 and 9** are directed to a computer-readable medium and an apparatus, and each are allowable for reasons similar to those discussed above with respect to Claim 1. Furthermore, Claim 9 recites “determining a hyperelliptic curve  $C$  of genus  $g$  over a field  $K$ , determining a Jacobian  $J(C)$  of the hyperelliptic curve  $C$ ” that is not taught or suggested by Frey1 or Frey2.

**Dependent Claims 2, 6, and 10** depend directly or indirectly from one of independent Claims 1, 5, and 9 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in Claim 1, are not taught, or suggested by Frey1 and Frey2.

#### The Cited Art Provides No Suggestion or Motivation to Modify or Combine the References

To establish a *prima facie* case of obviousness, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings (MPEP §2142). The Office stated the motivation for combining the methods of Frey1, and Frey2 is “because it would have been obvious to one of ordinary skill in the art to include a mathematical chain to reduce computation. However, there is nothing in either of the references that would suggest this motivation. The asserted motivation relies on hindsight

without evidence of teaching or suggestion to propose the suggested combination. Thus, this rejection is improper for this additional reason.

The Office Fails to Prove *Prima Facie* Case Of Obviousness

Applicant asserts the Office has failed to establish a *prima facie* case of obviousness. The Office cites official notice (page 5) without providing references but that elliptic curves and Tate Pairing have been very well known. Applicant respectfully challenges the Office to provide references.

Applicant respectfully submits that the cited references do not render the claimed subject matter obvious and that the claimed subject matter, therefore, patentably distinguishes over the cited references. For all of these reasons, Applicant respectfully requests the §103(a) rejection of these claims should be withdrawn.

**Claims 13-15, 17-32, 34-49, 51-63**

Applicant amends independent **Claims 13, 30, and 47** to recite features formerly recited in dependent Claims 16, 33, and 50, respectively. Accordingly, dependent Claims 16, 33, and 50 have been cancelled without prejudice.

As explained above with respect to the rejections above, Applicant submits that Frey1 and Frey2 fail to teach or suggest the features of independent Claims 1, 5, and 9. Also, there is no motivation to combine the two references. Furthermore, Barreto fails to compensate for the deficiencies of Frey1 and Frey2.

**Independent Claim 13** recites a method comprising:

determining a hyperelliptic curve  $C$  of genus  $g$  over a field  $K$  and a positive integer  $m$ ;

determining a Jacobian  $J(C)$  of the hyperelliptic curve  $C$ , and wherein each element  $D$  of  $J(C)$  contains a representative of the form  $A - g(P_0)$ , where  $A$  is an effective divisor of degree  $g$ ;

determining a plurality of functions  $h_{i,D}$  that are iterative building blocks for the formation of a function  $h_{m,D}$  in order to evaluate  $v_m$  which is a Squared Tate pairing;

outputting validation of selected information based on the Squared Tate pairing; and

determining a course of action in response to validation of selected information;

**wherein if  $P=(x, y)$  is a point on the hyperelliptic curve  $C$ , then  $-P$  denotes a point  $-P:=(x, -y)$ , and wherein if a point  $P=(x, y)$  occurs in  $A$  and  $y \neq 0$ , then  $-P := (x, -y)$  does not occur in  $A$  and a representative for identity will be  $g(P_0)$ .**

Applicant respectfully submits that no such method for is taught or suggested by Frey1, Frey2 and Barreto.

Frey1, Frey2, and Barreto, alone or in combination, do not teach or suggest "wherein if  $P=(x, y)$  is a point on the hyperelliptic curve  $C$ , then  $-P$  denotes a point  $-P:=(x, -y)$ , and wherein if a point  $P=(x, y)$  occurs in  $A$  and  $y \neq 0$ , then  $-P := (x, -y)$  does not occur in  $A$  and a representative for identity will be  $g(P_0)$ ", as recited in Applicant's Claim 1. The portions cited by the Office does not provide evidence illustrating these features are taught or suggested by these references.

**Independent Claims 30 and 47** are directed to a computer-readable medium and an apparatus, and each are allowable for reasons similar to those discussed above with respect to Claim 13.

**Dependent Claims 14-15, 17-29, 31-32, 34-46, and 48-63** depend directly or indirectly from one of independent Claims 13, 30, and 47 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited

features that, in combination with those recited in Claim 1, are not taught, or suggested by Frey1, Frey2, and Barreto.

Applicant respectfully submits that the cited references do not render the claimed subject matter obvious and that the claimed subject matter, therefore, patentably distinguishes over the cited references. For all of these reasons, Applicant respectfully requests the §103(a) rejection of these claims should be withdrawn.

### **Conclusion**

Claims 1, 2, 5, 6, 9, 10, 13-15, 17-32, 34-46, and 48-63 are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Office is requested to contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Lee & Hayes, PLLC  
421 W. Riverside Avenue, Suite 500  
Spokane, WA 99201

Dated: 9-28-07

By: Shirley Lee Anderson  
Shirley Lee Anderson  
Reg. No. 57,763  
(509) 324-9256 ext. 258